Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Об одном подходе к получению доступа к MacBook Pro с чипом T2 в рамках проведения криминалистической экспертизы

Хоруженко Георгий,
Passware

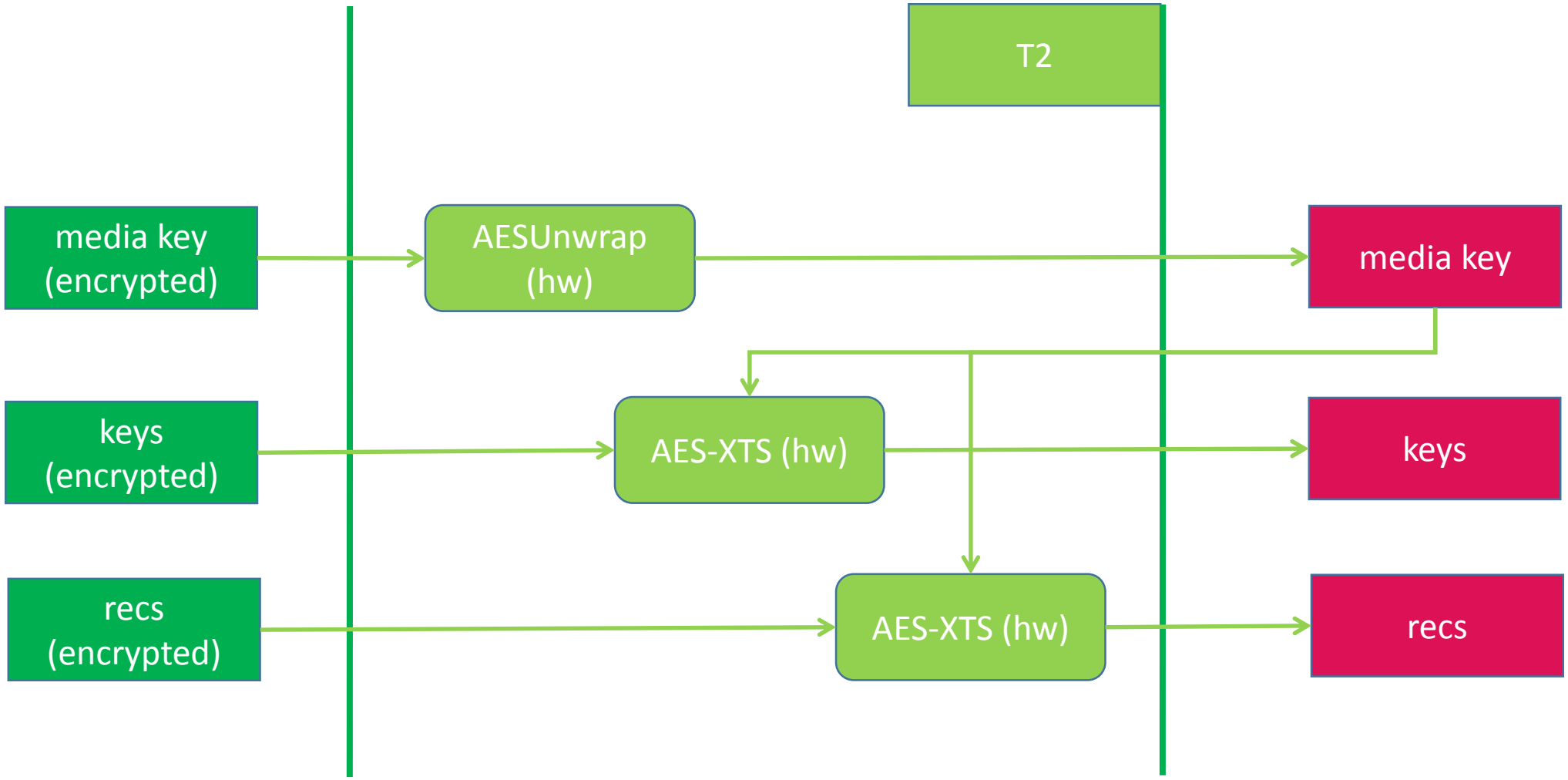
Актуальность

	Mac без чипа T2	Mac с чипом T2
Извлечение образа (в том числе, данных для проверки пароля)	+	?
Алгоритм проверки пароля	+	?
Алгоритм расшифрования защищенного раздела	+	?

Исходные данные

- Целевая машина – MacBook Pro 2018
- FileVault2 - включен
- T2 – blackbox

Данные для проверки пароля



Примеры идентификаторов ключей

- media key

```
0000000000: 61 B0 01 00 00 00 00 00  00 00 00 00 00 00 00 00  a°☺
0000000010: 84 CC 99 EC EF 62 FA 60  F7 C9 A5 04 4E E6 05 B4  „М™мпbъ` чЙГ♦Nж♣г
0000000020: EC 7E B5 54 63 6E FB B6  5D 13 57 F1 AC C3 D7 AC  м~µTcnы¶]‼Wc¬ГЧ¬
0000000030: 0B 19 62 1E AD 24 07 41  86 81 77 EE 94 75 EC BA  ♂↓b▲-$•A†Ѓwo”uмє
```

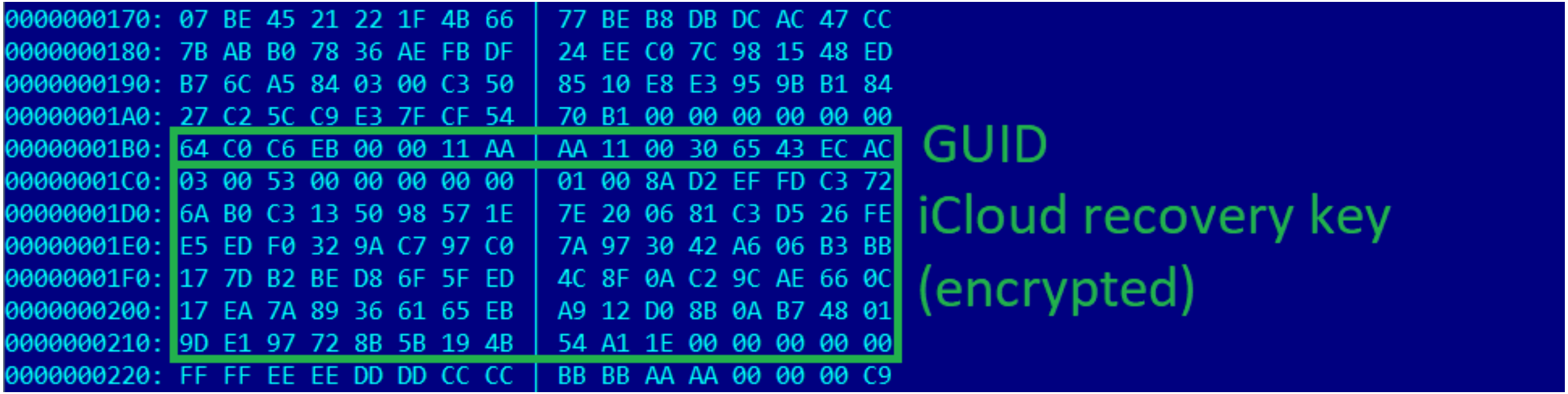
- volume key

```
0000000000: 61 B0 01 00 00 00 00 00  00 00 00 00 00 00 00 00  aA☺
0000000010: D1 78 D9 A7 6A F9 41 E5  D5 25 AF 93 F6 0A E5 78  бxйЇjљAхe%Ц▯i◙xx
0000000020: B8 8F 3A 2B A9 98 6C E0  27 B2 67 3C 06 D6 71 68  И▯:+Љ▯lр'Bg<♠жqh
0000000030: E0 EC 7C 1A 16 62 BC FD  22 40 EC 9E A4 0C D4 05  рь|→▬bM§"@ь▯Є♀д♣
```

iCloud key record

- Пароль для доступа к защищенному тому зашифрован на ключе из iCloud **(последний также попадает в iTunes backup):**

  6Q4X-Y6VG-HZ4C-MBXW-8PF5-53GE



Алгоритм действий

- Перевести целевую машину в **Target Disk Mode**, подключить кабелем **Thunderbolt 3** к рабочей машине (также **Mac**)
- Извлечь **iCloud key record**
- Расшифровать пароль с помощью iCloud account/**iTunes backup**
- Разблокировать защищенный раздел (**diskutil apfs unlockVolume**)

Более сложный случай

- **Target Disk Mode** недоступен:

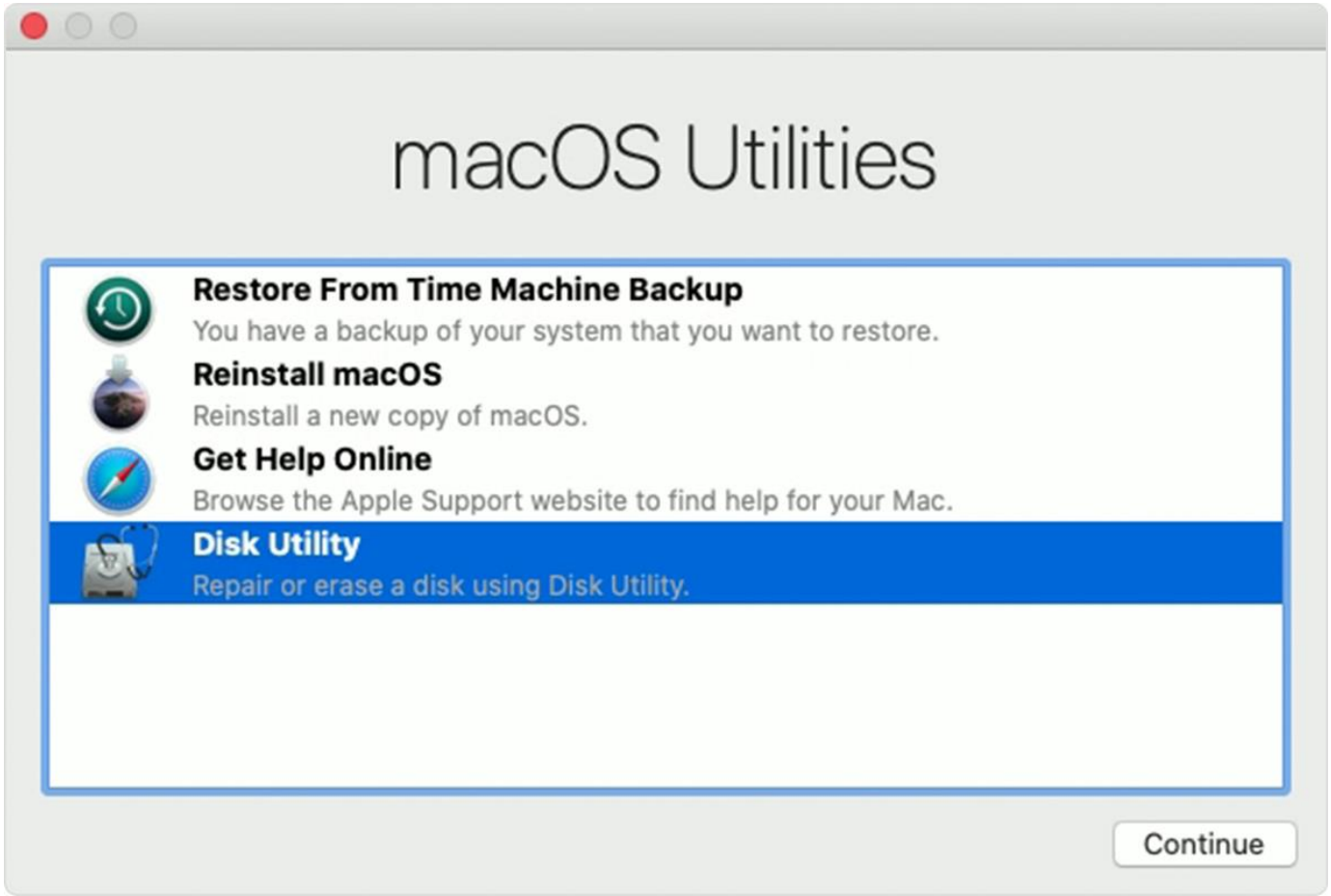
- повреждены порты целевой машины

- нет комплектующих (провод, Mac)

- …

- Возможно ли разблокировать раздел и извлечь данные в этом случае?

Recovery Mode (1)



Recovery Mode (2)

- На **macOS High Sierra**, **macOS Mojave** при загрузке в **Recovery mode** доступны приложения, в том числе **Safari**
- На **macOS Catalina** для доступа к приложениям нужно ввести пароль

Алгоритм действий

- Получить возможность выполнения кода в контексте **Safari**
- Загрузить и выполнить в памяти исполнимый Mach-O файл
- Повысить привилегии (**kernel**) и выйти за пределы текущего **sandbox**-профиля
- Отключить **SIP** (для загрузки произвольных расширений ядра)
- Запустить **reverse-shell** под пользователем **root**

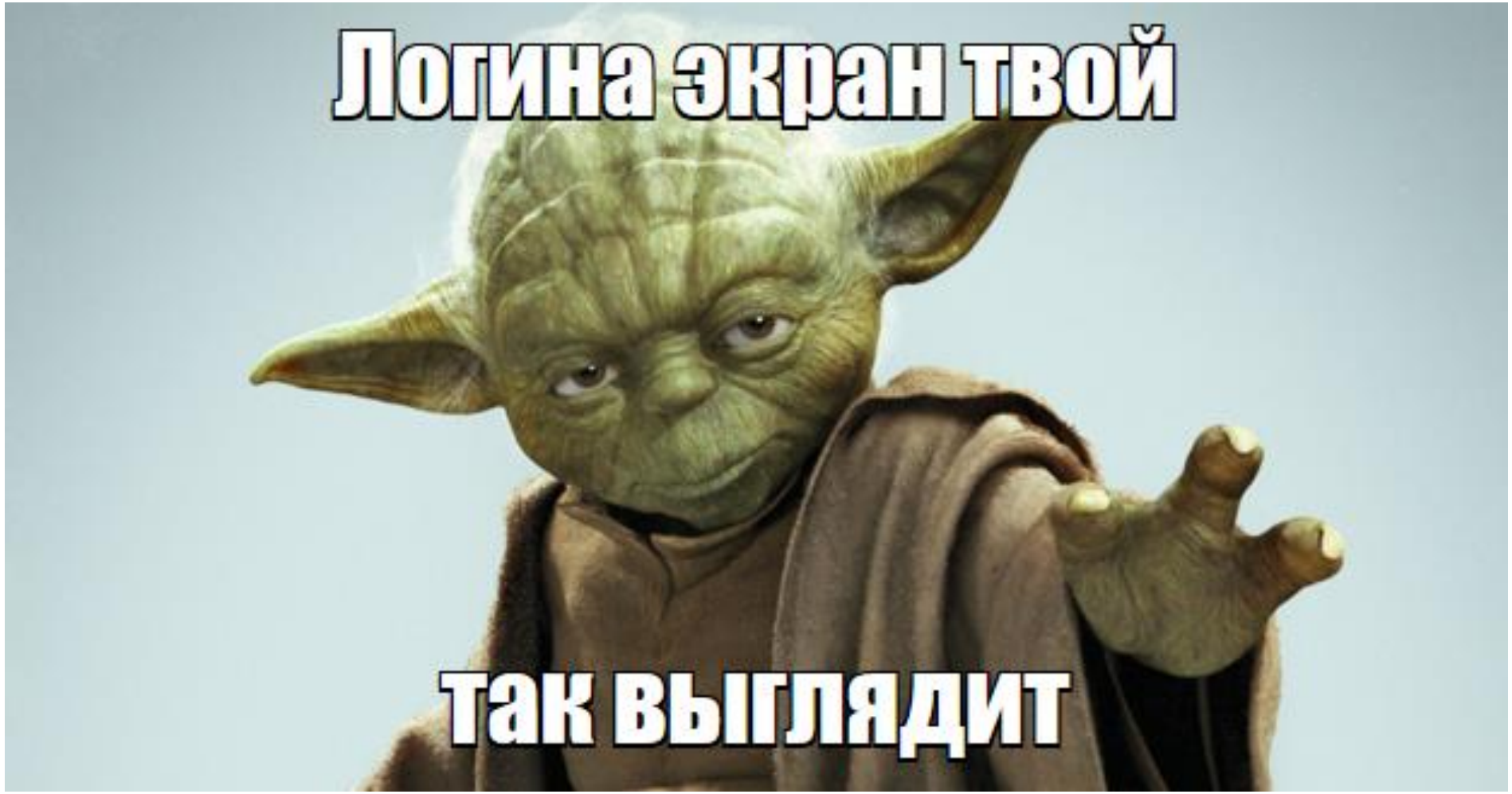
DEMO

Evil Maid (1)

- В результате возможно выполнение произвольного кода в контексте ядра целевой машины (без компрометации T2) … что открывает возможности для атаки в модели Evil Maid:

- загрузить приложение и модули ядра для ввода пользователем пароля и его проверки
- закрыть крышку MBP
- дождаться ввода пароля пользователем
- сохранить пароль на диске/отправить по сети

Evil Maid (2)



Результаты работы

- Предложен подход к получению доступа к заблокированному **MBP 2018** (с чипом **T2**) с помощью **iTunes backup** в двух случаях:

- через **Target Disk Mode**

- через эксплуатацию уязвимостей в **Safari** и ядре **macOS** в режиме **Recovery mode**

Контактная информация

Facebook:

facebook.com/passware

Сайт:

www.passware.com